AMENDMENTS TO THE CLAIMS

Please amend the claims by replacing the original claims with the following listing of claims.

LISTING OF THE CLAIMS:

1. (Currently amended) A method for securing, maintaining, monitoring and controlling computer files comprising:

providing a first data file, comprised of at least one first data file file name, as well as a first data file hash value, wherein said data file hash file is comprised of the contents of each file referred to by each of said first data file file names;

providing a second data file, comprised of at least one second data file file name;

comparing said second data file to said first data file in a comparison cycle, wherein said comparison cycle further comprises:

obtaining each file referred to by each of said second data file file names;

generating a second data file hash value <u>for each one of said second data file file names, or when the said file corresponding to the second data file file name does not exist providing notification of that</u>, wherein said data file hash file is comprised of the contents of each file referred to by each of said second data file file names;

sending each second data file hash value and each second data file file name to a comparison component.

2. (Original) A method as in claim 1 further comprising repeating the steps of: obtaining each file referred to by each of said second data file file names; generating a second data file hash value for each file referred to by each of said second data file file names; sending each second data file hash value and each second data file file name to a comparison component.

3. (Original) A method as in claim 1 further comprising the step of: comparing each second data file hash value to each first data file hash value.

4. (Previously presented) A method as in claim 1 wherein the step of providing a first data file further comprises proving a secure system data file.

5. (Previously presented) A method as in claim 1 wherein the step of providing a first data file further comprises proving an alternate data file.

6. (Original) A method as in claim 1 further comprising the step of reporting the results of said comparison cycle.

7. (Original) A method as in claim 1 further comprising the step of logging the results of said comparison cycle.

8. (Original) A method as in claim 1 further comprising the step of sending the results of said comparison cycle to a client comparison status mechanism.

9. (Original) A method as in claim 1 wherein the step of generating a first data file further comprises using a Loop Back mechanism to generate said first data file.

10. (Canceled)

11. (Canceled)

12. (Previously presented) A method as in claim 27 further comprising the step of reporting the results of said comparison cycle.

13. (Previously presented) A method as in claim 27 further comprising the step of logging the results of said comparison cycle.

14. (Previously presented) A method as in claim 27 further comprising the step of securing a system in lock down mode.

15. (Previously presented) A method as in claim 27 further comprising the step of sending the results of said comparison cycle to a client comparison status mechanism.

16. (Previously presented) A method as in claim 27 wherein the step of generating a secure system data file, further comprises using a Loop Back mechanism to generate said secure system data file.

17. (Canceled)

18. (Currently amended) An apparatus for securing, maintaining, monitoring and controlling computer files comprising:

a first data file, comprised of at least one first data file file name as well as a first data file hash value, wherein said data file hash file is comprised of the contents of each file referred to by each of said first data file file names;

a second data file, comprised of at least one second data file file name;

whereby said second data file is compared to said first data file, by: a means for obtaining each file referred to by each of said second data file file names,

a means for generating a second data file hash value for each one of said second data file file names, or when the said file corresponding to the second data file file name does not exist providing notification of that, wherein said data file hash file is comprised of the contents of each file referred to by each of said second data file file names; and,

a means for sending each second data file hash value and each second data file file name to a comparison component.

19. (Original) An apparatus as in claim 18 whereby said comparison component further comprises means for comparing each second data file hash value to each first data file hash value.

20. (Original) An apparatus as in claim 18 wherein said first data file further comprises a secure system data file.

21. (Original) An apparatus as in claim 18 wherein said first data file further comprises an alternate data file.

22. (Original) An apparatus as in claim 18 further comprising means for reporting the results of said comparison cycle.

23. (Original) An apparatus as in claim 18 further comprising means for logging the results of said comparison cycle.

24. (Original) An apparatus as in claim 18 further comprising means for sending the results of said comparison cycle to a client comparison status mechanism.

25. (Original) An apparatus as in claim 18 further comprising Loop Back mechanism means.

26. (Original) An apparatus as in claim 25 whereby said first data file is generated by said Loop Back mechanism means.

27. (Currently amended) A method for securing computer files comprising:

generating a secure system data file, further comprising creating a hash value for a file, wherein said first hash value is comprised of the contents of said file, and arranging said hash value with its respective file's name;

storing said secure system file; and,

comparing said secure system file to a comparison file in a comparison cycle, wherein said comparison file further comprises at least a second file, and wherein said comparison cycle further comprises hashing the contents of said second file, and sending said second hash value and its respective file's name to a comparison component, whereby said second file hash value is compared to said first file hash value, wherein records in the secure system data file have a one-to-one correspondence with the contents of the file, the file name, and the hash value of the contents of the file name.